

ENCRYPTION DEVICE USING DATA ENCRYPTION STANDARD ALGORITHM

Field of the Invention

5 The present invention relates to an encryption device; and, more particularly, to an encryption device using data encryption standard algorithm.

Prior Art of the Invention

10

DES (Data Encryption Standard) algorithm has come to the more attention in this environment of the wider usage of networks. Especially, the DES is widely used in Internet security applications, remote access server, cable modem or
15 satellite modem.

15

The DES is fundamentally a 64-bit block cipher having 64-bit block input and output, 56 bits among the 64-bit key block for encryption and decryption and remaining 8 bits for parity checking. And, the DES outputs a 64-bit plain text block and
20 a 64-bit cipher text generated from the input of the 56-bit key.

20

In a major technique, the DES is implemented by permutation (P-Box), substitution (S-Box) and key schedule generating sub-key.

25

Inside of data encryption is implemented in such a way to iteration of 16 round operations and constructed by an initial permutation (IP) of input part and an inverse initial

permutation (IP^{-1}) of output part.

Fig. 1 is a detailed diagram of the cipher function and the S-Box permutation unit of a general DES architecture.

Referring to Fig. 1, the cipher function f includes an
5 expansion permutation unit 110, an exclusive-OR (XOR) unit 120, an S-Box permutation unit 130, a P-Box permutation unit 140 and an XOR unit 150.

The expansion permutation unit 110 performs expansion permutation over 32-bit data ($R_{(i-1)}$) from a right register
10 registering 32-bit text block to output 48-bit data.

The XOR unit 120 performs XOR operation over the 48-bit data from the expansion permutation unit 110 and a sub-key (K_i) from a key scheduler.

The S-Box permutation unit 130 performs substitution over
15 48-bit data from the XOR unit 120 to output 32-bit data.

The P-Box permutation unit 140 performs permutation over 32-bit data from the S-Box permutation unit 130.

The XOR unit 150 performs XOR operation over 32-bit data from the P-Box permutation unit 140 and 32-bit data ($L_{(i-1)}$)
20 from a left register.

The key scheduler includes two shift units 160 and 170 and a compression permutation unit 180. Each of the shift units 160 and 170 respectively shifts corresponding 28 bits, half of 56-bit key data.

25 The compression permutation unit 180 receives two blocks from the shift units 160 and 170 to compress them to the sub key.

In particular, the S-Box permutation unit 130 includes 8 S-Boxes for receiving 48-bit data and outputting 32-bit data. That is, 48-bit data block is divided into 8 6-bit data, each applied to the corresponding S-Box of the 8 S-Boxes and each of the 8 S-Boxes outputs 4-bit data. Accordingly, 48-bit data is permuted to 32-bit data. The S-Box permutation unit 130 requires a memory, e.g., a programmable logic array (PLA) or a read only memory (ROM), because it employs table look-up technique. Since each of the S-Boxes outputs 4 bits for 6-bit input, it requires 64 x 4 memory capability and the S-Box permutation unit 130 requires 8 x 64 x 4 memory capability. Accordingly, the S-Box permutation unit 130 takes relatively large area in a chip.

Fig. 2 is a block diagram of a DES architecture having 4-stage pipeline structure using a 2 phases clock, which has an effect on processing capability and is applied to an embodiment of the present invention.

Referring to Fig. 2, in the DES algorithm, 64-bit plain text block undergone an IP unit is divided into two blocks, a_0 and b_0 . The a_0 and b_0 are respectively registered at a first left register (A0) 290 and a first right register (B0) 200 by using a first clock (CLK1) and a second clock (CLK2).

32-bit data registered at the first right register (B0) 200 is encrypted by the cipher function f_B 210 using the sub-key ($K_{(i)}$) from the key scheduler and the encrypted 32-bit data is X-ORed with the 32-bit data registered at the first left register (A0) 290 at the X-OR unit 220. 32-bit data from the

X-OR unit 220 is registered at a second left register (A1) 230 by using a first clock (CLK1).

32-bit data registered at the second left register (A1) 230 is encrypted by the cipher function f_c 240 using the sub-
5 key ($K_{(i+1)}$) from the key scheduler and the encrypted 32-bit data is X-ORed with the 32-bit data registered at the first right register (B0) 200 at the X-OR unit 250. 32-bit data from the X-OR unit 250 is registered at a second right register (B1) 260 by using the second clock (CLK2).

10 32-bit data registered at the second right register (B1) 260 is encrypted by the cipher function f_D 270 using the sub-key ($K_{(i+2)}$) from the key scheduler and the encrypted 32-bit data is X-ORed with the 32-bit data registered at the second left register (A1) 230 at the X-OR unit 280. 32-bit data from
15 the X-OR unit 280 is registered at the first left register (A0) 290 by using the first clock (CLK1).

32-bit data registered at the first left register (A0) 290 is encrypted by the cipher function f_A 300 using the sub-
20 key ($K_{(i+3)}$) from the key scheduler and the encrypted 32-bit data is X-ORed with the 32-bit data registered at the second right register (B1) 260 at the X-OR unit 310. 32-bit data from the X-OR unit 310 is registered at the first right register (B0) 200 by using the second clock (CLK2).

At a final round, 32-bit of the first left register (A0) 25 290 becomes block b_{15} and 32-bit from the X-OR unit 310 becomes b_{16} .

The second clock (CLK2) is a delayed version of the first

clock (CLK1) by 1/2 period. At a rising edge of the first clock (CLK1), new data are registered at the register A0 and A1. At a rising edge of the second clock (CLK2), new data are registered at the register B0 and B1.

5 Fig. 3 is a timing diagram for explaining operation of the DES architecture having the 4-stage pipeline structure in Fig. 2.

Referring to Fig. 3, 32-bit data blocks a_0 and b_0 are generated by dividing initial-permuted 64-bit plain text block to two 32-bit blocks and a_0 and b_0 are respectively registered at registers A0 and B0 at t_0 of the first clock (CLK1) and t_1 of the second clock (CLK2). Computation of b_1 ($b_1 = a_0 \oplus f(b_0, K_1)$) is started from t_1 and the computed value is registered at the register A1 at t_2 . Because the registers A0 and B0 are registered by the first clock (CLK1) and the second clock (CLK2) which are delayed from each other, a_0 registered at the register A0 remains to t_2 so that a_0 can be used to compute b_1 at t_1 - t_2 period. b_1 is remained to t_4 so that b_1 can be used to compute b_2 at t_2 - t_4 period. In other words, times which the left registers register new data are t_0, t_2, t_4, \dots , and times which the right registers register new data are t_1, t_3, t_5, \dots .

Because b_0 registered in the register B0 at t_1 and b_1 registered in the register A1 at t_2 remains to t_2 - t_3 , b_2 ($b_2 = b_0 \oplus f(b_1, K_2)$) is computed at t_2 - t_3 period and registered at the register B1 at t_4 by the second clock (CLK2). Computed values b_3, b_7, b_{11}, b_{15} are registered in the first left register (A0)

at rising edges of the first clock (CLK1), t_4 , t_8 , t_{12} , t_{16} , and computed values b_5 , b_9 , b_{13} are registered in the second left register (A1) at rising edges of the first clock (CLK1), t_6 , t_{10} , t_{14} . Similarly, computed values b_4 , b_8 , b_{12} , b_{16} are registered in the first right register (B0) at rising edges of the second clock (CLK2), t_5 , t_9 , t_{13} , t_{17} , and computed values b_6 , b_{10} , b_{14} are registered in the second register (B1) at rising edges of the second clock (CLK2), t_7 , t_{11} , t_{15} .

As described above, by accessing stored values at the registers simultaneously using the clock having 2 phases, the computation time for b_1 , b_2 , . . . , b_{16} can be reduced to 8.5 cycles.

Typically, for a given key, 64-bit plain text or cipher text blocks to be encrypted or decrypted are applied continuously. For example, because an encryption technique for use in MCNS cable modem performs encryption in unit of MAC frame, at most 1,518 bytes plain text blocks are encrypted by using an identical key. That is, 16 round DES cores should be computed a number of plain text blocks by using the identical key. In this case, the pipeline structure can increase the processing capability.

Fig. 4 is a timing diagram for explaining operation of pipeline of the DES architecture having the conventional 4-stage pipeline structure in Fig. 2.

Referring to Fig. 4, by using the pipeline structure, two plain text blocks can be processed during 8.5 cycles. And, inserting new plain text blocks c_0 and d_0 to the registers A0

and B0 at t_2 and t_3 during a vacant period in Fig. 3, the plain text block d_i can be computed while computation of the plain text block b_i . In order to encrypt new plain text blocks b_i and d_i during every period $t_0 - t_1$, $t_1 - t_2$, . . . , two cipher functions are performed simultaneously for every period. The number of the plain text blocks that can be processed within 8.5 cycles can be increased by two times. However, the S-Box forming the cipher function should be added.

Referring to Fig. 2 again, it shows a timing diagram for explaining operations of the cipher function when the pipeline of the DES architecture having the conventional 4-stage pipeline structure is not used and when the pipeline is used.

In case that one 64-bit plain text block is encrypted, i.e., the pipeline is not used, the cipher functions f_A , f_B , f_C , f_D can be implemented by one S-Box permutation unit because the computation of them are performed time-divisionally by the clock having 2 phases. However, because (f_A, f_C) and (f_B, f_D) are not time divided while (f_A, f_B) and (f_C, f_D) is timely divided when the two plain text blocks are encrypted simultaneously, two S-Box are required.

Fig. 5 is a detailed block diagram of a conventional single port S-Box permutation unit.

Referring to Fig. 5, conventionally, the pipeline operation is performed by using the two S-Box permutation units and each of the S-Box permutation units includes 8 S-Boxes, input and output of each S-Box being 48-bit data and 32-bit, respectively. Each S-Box is formed by 64 x 4 ROM or

PLA and has a path receiving 6-bit address and outputting 4-bit data. Accordingly, there are provided two physically separated paths, a first path and a second path, by the two S-Box permutation units.

5 Fig. 6 is a block diagram of a DES architecture having 8-stage pipeline structure using a 2 phases clock, which has an effect on processing capability and is applied to other embodiments of the present invention.

Referring to Fig. 6, in the DES algorithm, 64-bit plain
10 text block undergone an IP unit is divided into two blocks, a_0 and b_0 . The a_0 and b_0 are respectively registered at a first left register (A0) 660 and a first right register (B0) 600 by using a first clock (CLK1) and a second clock (CLK2).

32-bit data registered at the first right register (B0)
15 600 is encrypted by the cipher function f_B 610 using the sub-key ($K_{(i)}$) from the key scheduler and the encrypted 32-bit data is X-ORed with the 32-bit data registered at the first left register (A0) 660 at the X-OR unit 620. 32-bit data from the X-OR unit 620 is registered at a second left register (A1) 630
20 by using a first clock (CLK1).

32-bit data registered at the second left register (A1)
630 is encrypted by the cipher function f_C 640 using the sub-key ($K_{(i+1)}$) from the key scheduler and the encrypted 32-bit data is X-ORed with the 32-bit data registered at the first
25 right register (B0) 600 at the X-OR unit 650. Two rounds as described above are iterated, at a final round, 32-bit of the first left register (A0) 660 becomes block b_{15} and 32-bit from

the X-OR unit 670 becomes b_{16} .

A1, A2, A3 and A0 denote the left registers, and B1, B2, B3 and B0 denote the right registers. At a rising edge of the first clock (CLK1), new data are registered at the register
5 A0, A1, A2 and A3. At a rising edge of the second clock (CLK2), new data are registered at the register B0, B1, B2 and B3.

The second clock (CLK2) is an inverse clock and a delayed version of the first clock (CLK1) by $1/2$ period.

10 Fig. 7 is a timing diagram for explaining operation of the DES architecture having the 8-stage pipeline structure in Fig. 6.

Referring to Fig. 7, 32-bit blocks a_0 and b_0 are generated by dividing initial-permuted 64-bit plain text block to two
15 32-bit blocks and a_0 and b_0 are respectively registered at registers A0 and B0 at t_0 of the first clock (CLK1) and t_1 of the second clock (CLK2). Computation of b_1 ($b_1 = a_0 \oplus f(b_0, K_1)$) is started from t_1 and the computed value is registered at the register C0 at t_2 . Because the registers A0 and B0 are
20 registered by the first clock (CLK1) and the second clock (CLK2) which are delayed from each other, a_0 registered at the register A0 remains to t_2 so that a_0 can be used to compute b_1 at t_1 - t_2 period. b_1 is remained to t_4 so that b_1 can be used to compute b_2 at t_2 - t_1 period. In other words, times the second
25 left register (A1) registers new data are t_0, t_2, t_4, \dots , and times the first right register (B0) registers new data are t_1, t_3, t_5, \dots .

Because b_0 registered in the register B0 at t_1 and b_1 registered in the register A1 at t_2 remains to t_2-t_3 , b_2 ($b_2 = b_0 \oplus f(b_1, K_2)$) is computed at t_2-t_3 period and registered at the register B1 at t_4 by the second clock (CLK2).

5 Computed values a_0 , b_7 , b_{15} are registered in the first left register (A0) at rising edges of the first clock (CLK1), t_0 , t_8 , t_{16} , computed values b_1 and b_9 are registered in the second left register (A1) at rising edges of the first clock (CLK1), t_2 and t_{10} , computed values b_3 and b_{11} are registered in
10 the third left register (A2) at rising edges of the first clock (CLK1), t_4 and t_{12} , and computed values b_6 and b_{14} are registered in the fourth left register (A2) at rising edges of the first clock (CLK1), t_6 and t_{14} .

Similarly, computed values b_0 , b_8 , b_{16} are registered in
15 the first right register (B0) at rising edges of the second clock (CLK2), t_1 , t_9 , t_{17} , computed values b_2 , b_{10} are registered in the second register (B1) at rising edges of the second clock (CLK2), t_3 , t_{11} , computed values b_4 , b_{12} are registered in the third register (B2) at rising edges of the second clock
20 (CLK2), t_5 , t_{13} , and computed values b_6 , b_{14} are registered in the fourth register (B2) at rising edges of the second clock (CLK2), t_7 , t_{15} .

Fig. 8 is a timing diagram for explaining operation of pipeline of the DES architecture having the 8-stage pipeline
25 structure in Fig. 6.

Referring to Fig. 6, by using the pipeline structure, four plain text blocks can be processed during 8.5 cycles. And,

inserting new plain text blocks c_0 and d_0 to the registers A0 and B0 at t_2 and t_3 , e_0 and f_0 at t_4 and t_5 , g_0 and h_0 at t_6 and t_7 , during a vacant period in Fig. 7, the plain text block d_i , f_i , h_i can be computed while computation of the plain text block b_i . In order to encrypt new plain text blocks b_i , d_i , f_i and h_i during every period $t_0 - t_1$, $t_1 - t_2$, $t_2 - t_3$, . . ., four cipher functions are performed simultaneously for every period. The number of the plain text blocks that can be processed within 8.5 cycles can be increased by four times.

10 However, three S-Box permutation units should be added.

Referring to Fig. 9, it shows a timing diagram for explaining operations of the cipher function when the pipeline of the DES architecture having the 8-stage pipeline structure is not used and when the pipeline is used.

15 In case that one 64-bit plain text block is encrypted, i.e., the pipeline is not used, the cipher functions f_A , f_B , f_C , f_D , f_E , f_F , f_G , f_H can be implemented by one S-Box permutation unit because the computation of them are performed time-divisionally by the clock having 2 phases. However, 20 because (f_A, f_C, f_E, f_G) and (f_B, f_D, f_F, f_H) are not time divided while (f_A, f_B, f_C, f_D) and (f_E, f_F, f_G, f_H) is timely divided when the four plain text blocks are encrypted simultaneously, four S-Boxes are required.

Fig. 10 is a detailed block diagram of a conventional 25 single port S-Box permutation unit.

Referring to Fig. 10, conventionally, the pipeline operation is performed by using the four S-Box permutation

units and each of the S-Box permutation units includes 8 S-Boxes, input and output of each S-Box being 48-bit data and 32-bit, respectively. Each S-Box is formed by 64 x 4 ROM or PLA and has a path receiving 6-bit address and outputting 4-bit data. Accordingly, there are provided four physically separated paths, a first path, a second path, a third path and a fourth path, by the four S-Box permutation units.

As described above, conventionally, a problem of an access to the memory required for the S-Box permutation unit, i.e., a data contention problem, is solved by the two physically separated paths of the two S-Box permutation units. However, since the two identical S-Box permutation units are used, area is increased.

Summary of the Invention

Therefore, it is an object of the present invention to provide an encryption device eliminating data contention and minimizing area that can access data multiple times within a given time.

It is another object of the present invention to provide an encryption device reducing a chip size and increasing its performance.

In accordance with an aspect of the present invention, there is provided an encryption device for performing encryption of plain text blocks using data encryption standard algorithm, wherein the encryption device includes an initial

permutation unit, a data encryption unit having n-stage (n is an even number equal to or larger than four) pipeline structure using a first clock and a second clock and an inverse initial permutation unit, the encryption device
5 comprising: a multiplexer for selecting one of a half of n 48-bit inputs; 8 S-Boxes, each for receiving 6-bit address among the selected 48-bit and outputting 4-bit data; a demultiplexer for distributing 4-bit data from each of the S-Boxes to the half of n outputs; and a controller for control the
10 multiplexer and the demultiplexer with the first clock and the second clock.

In accordance with another aspect of the present invention, there is provided an encryption device for performing encryption of plain text blocks using data
15 encryption standard algorithm, wherein the encryption device includes an initial permutation unit, a data encryption unit having 8-stage pipeline structure using a first clock and a second clock and an inverse initial permutation unit, the encryption device comprising: a first multiplexer for
20 selecting one of a first and a second 48-bit inputs; a first S-Box unit having 8 S-Boxes, each S-Box for receiving 6-bit address among selected 48-bit from the first multiplexer and outputting 4-bit data; a first demultiplexer for distributing 4-bit data from each of the S-Boxes to one of a first and a
25 second outputs; a first controller for controlling the first multiplexer and the first demultiplexer with a third clock and a fourth clock; a second multiplexer for selecting one of a

third and fourth 48-bit inputs; a second S-Box unit having 8 S-Boxes, each S-Box for receiving 6-bit address among selected 48-bit from the second multiplexer and outputting 4-bit data; a second demultiplexer for distributing 4-bit data from each of the S-Boxes to one of a third and a fourth outputs; and a second controller for controlling the second multiplexer and the second demultiplexer with the third clock and the fourth clock, wherein the third and the fourth clocks are faster than the first and the second clocks by two times.

Brief Description of the Drawings

The above and other objects and features of the instant invention will become apparent from the following description of preferred embodiments taken in conjunction with the accompanying drawings, in which:

Fig. 1 is a cipher function and a S-Box permutation unit having a general DES architecture;

Fig. 2 is a block diagram of DES architecture having 4-stage pipeline structure using a 2 phases clock, which has an effect on processing capability and is applied to an embodiment of the present invention;

Fig. 3 is a timing diagram for explaining operation of the DES architecture having the 4-stage pipeline structure in Fig. 2;

Fig. 4 is a timing diagram for explaining operation of pipeline of the DES architecture having the 4-stage pipeline

structure in Fig. 2;

Fig. 5 is a detailed block diagram of a conventional single port S-Box permutation unit;

Fig. 6 is a block diagram of DES architecture having 8-stage pipeline structure using a 2 phases clock, which has an effect on processing capability and is applied to other embodiment of the present invention;

Fig. 7 is a timing diagram for explaining operation of the DES architecture having the 8-stage pipeline structure in Fig. 6;

Fig. 8 is a timing diagram for explaining operation of pipeline of the DES architecture having the 8-stage pipeline structure in Fig. 6;

Fig. 9 is a diagram illustrating a timing diagram for explaining operations of the cipher function when the pipeline of the DES architecture having the 8-stage pipeline structure is not used and when the pipeline is used;

Fig. 10 is a block diagram of a conventional single port S-Box permutation unit;

Fig. 11 is a detailed block diagram of 2-port S-Box permutation in accordance with an embodiment of the present invention;

Fig. 12 is a timing diagram for explaining operation of the conventional single port S-Box permutation unit and the 2-port S-Box permutation unit of the present invention;

Fig. 13 is a detailed block diagram of 4-port S-Box permutation in accordance with another embodiment of the

present invention;

Fig. 14 is a timing diagram for explaining operation of the conventional single port S-Box permutation unit and the 4-port S-Box permutation unit of the present invention;

5 Fig. 15 is a detailed block diagram of two 2-port S-Box permutation in accordance with further another embodiment of the present invention; and

10 Fig. 16 is a timing diagram for explaining operation of the conventional single port S-Box permutation unit and two 2-port S-Box permutation unit of the present invention.

Preferred Embodiment of the Invention

15 Hereinafter, preferred embodiments of the present invention will be described in detail with reference to the accompanying drawings.

Embodiment 1

20 Fig. 11 is a detailed block diagram of 2-port S-Box permutation in accordance with the present invention.

Referring to Fig. 11, a S-Box permutation unit includes a multiplexer 1110, 8 S-Boxes 1120, a demultiplexer 1130 and a controller 1140. The multiplexer 1110 selects one of two 48-bit inputs under control of the controller 1140. Each of the S-Boxes 1120 receives 6-bit address among the selected 48-bit and outputs 4-bit data. The demultiplexer 1130 distributes

the 4-bit data from each of the S-Boxes 1120 to two outputs under control of the controller 1140. The controller 1140 controls the multiplexer 1110 and the demultiplexer 1130 with a first clock (CLK_A) and a second clock (CLK_B).

5 Fig. 12 is a timing diagram for explaining operation of the conventional single port S-Box permutation unit and the 2-port S-Box permutation unit.

Referring to Fig. 12, in the present invention, signals required to access ROM are generated by using the first clock (CLK_A) and the second clock (CLK_B) that are faster than input clocks (CLK_1, CLK_2) by two times. The data contention problem is eliminated since there exist a first path (path1) and a second path (path2) those are timely divided by the multiplexer selecting one of the first path (path1) and the second path (path2) at each time period $t_i - t_{i+1}$. That is, when the first clock (CLK_A) is logic high, the first path (path1) is selected and b_i are computed and when the second clock (CLK_B) is logic high, the second path (path2) is selected and d_i are computed.

20 As described above, by using only one S-Box, the present invention can reduce area of the S-Box permutation unit to a half so that circuits can be efficiently disposed, i.e., the number of net die is increased in smaller chip area so that cost is decreased.

25

Embodiment 2

Fig. 13 is a detailed block diagram of 4-port S-Box permutation in accordance with another embodiment of the present invention.

Referring to Fig. 13, a S-Box permutation unit includes a multiplexer 1310, 8 S-Boxes 1320, a demultiplexer 1330 and a controller 1340. The multiplexer 1310 selects one of four 48-bit inputs under control of the controller 1340. Each of the S-Boxes 1320 receives 6-bit address among the selected 48-bit and outputs 4-bit data. The demultiplexer 1330 distributes the 4-bit data from each of the S-Boxes 1320 to two outputs under control of the controller 1340. The controller 1340 controls the multiplexer 1310 and the demultiplexer 1330 with a first clock (CLK_A) and a second clock (CLK_B).

Fig. 14 is a timing diagram for explaining operation of the conventional single port S-Box permutation unit and the 2-port S-Box permutation unit.

Referring to Fig. 14, in the present invention, signals required to access ROM are generated by using the first clock (CLK_A) and the second clock (CLK_B) that are faster than input clocks (CLK_1, CLK_2) by four times. The data contention problem is eliminated since there exist a first path (path1), a second path (path2), a third path (path3) and a fourth path (path4) those are timely divided by the multiplexer selecting one of the first path (path1), the second path (path2), the third path (path3) and the fourth path (path4) at each time period $t_i - t_{i+1}$. The controller generates signals necessary to access the ROM based on the first and the second clock (CLK_A,

CLK_B).

As described above, by using only one S-Box, the present invention can reduce area of the S-Box permutation unit to 1/4 so that circuits can be efficiently disposed, i.e., the number of net die is increased in smaller chip area so that cost is decreased.

The S-box in accordance with this embodiment has smaller size than the conventional S-box illustrated in Fig. 10. However, access rate of the S-box in this embodiment is slower than that of the S-box illustrated in Fig. 10.

Embodiment 3

In this embodiment, when the S-Box cannot be implemented by using faster storage device by four times, a S-Box permutation unit is implemented by two 2-port S-Boxes by using storage device two times faster than that of the S-box illustrated in Fig. 10.

Referring to Fig. 15, each of two S-Box permutations unit includes a multiplexer 1510 or 1550, 8 S-Boxes 1520 or 1560, a demultiplexer 1530 or 1570, and a controller 1540 or 1580. A first multiplexer 1510 selects one of two 48-bit inputs under control of the controller 1540. Each of first S-Boxes 1520 receives 6-bit address among the selected 48-bit and outputs 4-bit data. A first demultiplexer 1530 distributes the 4-bit data from each of the S-Boxes 1520 to two outputs under control of the controller 1540. The

controller 1540 controls the multiplexer 1510 and the demultiplexer 1530 with a first clock (CLK_A) and a second clock (CLK_B). A second multiplexer 1550 selects one of two 48-bit inputs under control of the controller 1580. Each of 5 second S-Boxes 1560 receives 6-bit address among the selected 48-bit and outputs 4-bit data. A second demultiplexer 1570 distributes the 4-bit data from each of the S-Boxes 1560 to two outputs under control of the controller 1580. The controller 1580 controls the multiplexer 1550 and the 10 demultiplexer 1570 with a first clock (CLK_A) and a second clock (CLK_B).

Fig. 16 is a timing diagram for explaining operation of the conventional single port S-Box permutation unit and the 2-port S-Box permutation unit.

15 Referring to Fig. 16, in the present invention, signals required to access ROM are generated by using the first clock (CLK_A) and the second clock (CLK_B) that are faster than input clocks by two times. The data contention problem is eliminated since there exist a first path (path1) and a second 20 path (path2) those are timely divided by the multiplexer selecting one of the first path (path1) and the second path (path2) at each time period $t_i - t_{i+1}$. That is, when the first clock (CLK_A) is logic high, the first path (path1) and the third path (path3) are selected and b_i and f_i are computed and 25 when the second clock (CLK_B) is logic high, the second path (path2) and the fourth path (path4) are selected and d_i and h_i

are computed.

While the present invention has been shown and described
with respect to the particular embodiments, it will be
apparent to those skilled in the art that many changes and
5 modifications may be made without departing from the spirit
and scope of the invention as defined in the appended claims.

11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208
2209
2210
2211
2212
2213
2214
2215
2216
2217
2218
2219
2220
2221
2222
2223
2224
2225
2226
2227
2228